WHAT IS CLAIMED IS:

1. A system comprising:

a communications engine for establishing a communications link with a client;

security means coupled to the communications engine for determining client privileges;

a servlet host engine coupled to the security means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and

a keysafe for storing a key which enables access to the secured service.

2. The system of claim 1, wherein the communications engine uses SSL technology to create a secure communications link with the client.

3. The system of claim 1, wherein communications engine negotiates an encryption protocol for transferring messages to and from the client.

4. The system of claim 1, wherein the communications engine uses public key certificates for transferring messages to and from the client.

5. The system of claim 1, wherein the security means uses public key certificates to authenticate the client.

6. The system of claim 1, wherein the security means examines client identity and the level of authentication to determine client privileges.

7. The system of claim 1, wherein the security means examines a global certificate to authenticate the client.

8. The system of claim 1, wherein the security means uses digital signature technology to authenticate the client.

9. The system of claim 1, wherein the servlet host engine forwards to the client a security applet for enabling the client to perform a security protocol recognized by the security means.

10. The system of claim 1, wherein the service is secured by a corporate firewall and the key is configured to enable communication through the firewall.

11. The system of claim 1, further comprising a global firewall for protecting the system.

12. The system of claim 1, further comprising a service address for identifying the location of the secured service.

13. The system of claim 1, wherein the applet provides to the client a direct connection with the secured service.

14. The system of claim 1, further comprising a proxy in communication with the secured service, and wherein the applet enables I/O with the proxy.

15. A method comprising the steps of:

establishing a communications link with a client;

determining client privileges;

providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and

retrieving a key which enables access to the secured service.

16. The method of claim 15, wherein establishing a communications link includes the step of using SSL technology to create a secure communications link with the client.

17. The method of claim 15, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

18. The method of claim 15, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

19. The method of claim 15, wherein determining client privileges includes the step of using public key certificates to authenticate the client.

20. The method of claim 15, wherein determining client privileges includes the step of examining client identity and the level of authentication to determine client privileges.

21. The method of claim 15, wherein determining client privileges includes the step of examining a global certificate to authenticate the client.

22. The method of claim 15, wherein determining client privileges includes the step of using digital signature technology to authenticate the client.

23. The method of claim 15, wherein establishing a communications link includes forwarding to the client a security applet for enabling the client to perform a recognized security protocol.

24. The method of claim 15, further comprising the step of using the key to communicate through a firewall to the secured service.

25. The method of claim 15, wherein the method is performed by a global server and further comprising using a global firewall to protect the global server.

26. The method of claim 15, further comprising using a service address to identify the location of the secured service.

27. The method of claim 15, wherein providing includes the step of providing to the client a direct connection with the secured service.

28. The method of claim 15, further comprising using a proxy in communication with the secured service, and wherein providing includes enabling I/O with the proxy.

29. A system comprising:

means for establishing a communications link with a client;

means for determining client privileges;

means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and

means for retrieving a key which enables access to the secured service.

30. A computer-based storage medium storing a program for causing a computer to perform the steps of:

establishing a communications link with a client;

determining client privileges;

providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and

retrieving a key which enables access to the secured service.